



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/657,122	09/07/2000	Pau-Chen Cheng	AUS9-2000-0479-US1	2397

7590

04/19/2004

Kelly K Kordzik  
Suite 800  
100 Congress Avenue  
Austin, TX 78701

EXAMINER

BAUM, RONALD

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 04/19/2004

4

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/657,122

Applicant(s)

CHENG ET AL.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 18 February 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,2,5-48 and 51-70 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 19-24,41-46 and 65-70 is/are allowed.
- 6) ☒ Claim(s) 1,2,5-18,25-40,47,48 and 51-64 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 09/07/2000.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. This action is in reply to applicant's correspondence of 18 February 2004.
2. Claims 1,2,5-18,25-40,47,48 and 51-64 remain rejected under 35 U.S.C. 103(a).  
Claims 19-24,41-46, and 65-70 are objected to.

#### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1,2,5-9,12,16,25-31,34,38,47-48,51-55,58,62 are rejected under 35 U.S.C. 102(b) as being anticipated by Bots et al, U.S. Patent 6,226,748 B1.

4. As per claim 1 ; “A method for allowing a server node in a virtual private network [figure 2, col. 2,lines 44-54, col. 4,lines 67-col. 5,line 3, col. 5,lines 61-col. 6,line 37] to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of: configuring [col. 4,lines 3-27, the VPN server functions are either hardware or hardware/software combinations, such that the *configuration* of such (i.e., via the computer operating system utilizing appropriate resident or loadable applications) would be an inherent computer function associated with the computer part of the VPN server] a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name [col. 6,lines 34-36, col.

Art Unit: 2136

8,lines 15-33]; configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name [col. 2, lines 55-65, col. 7,lines 20-55, col. 8,lines 5-15]; establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group.”;

And further as per claim 25; “A network system [This claim is the apparatus of method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above, where the Bots et al invention is clearly a network system (i.e., col. 4,lines 15-27)] comprising: a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises: a group database, wherein said group database comprises said group name and a list of members associated with said group name; and a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name.”;

And further as per claim 47; “A computer program product having a computer readable medium having computer program logic recorded thereon [This claim is the software embodied on computer readable media for the method of claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising: programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name; programming operable for establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and programming operable for associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group.”.

5. Claim 2 *additionally recites* the limitations that “The method as recited in claim 1 further comprising the step of configuring a tunnel definition database in said server node, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.”.

Art Unit: 2136

The teachings of Bots et al (col. 7, lines 4-19, lines 32-39, lines 55-col. 8, line 4) suggest such limitations;

And further as per claim 26; "The network system as recited in claim 25 [This claim is the apparatus of method claim 2, and is rejected for the same reasons provided for the claim 2 rejection above], wherein said server node further comprises: a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.";

And further as per claim 48; "The computer program product as recited in claim 47 [This claim is the software embodied on computer readable media for the method of claim 2, and is rejected for the same reasons provided for the claim 2 rejection above] further comprises: programming operable for configuring a tunnel definition database in said server node, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.".

6. And further as per claim 27; "The network system [This claim is the apparatus of method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above] as recited in claim 26, wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name.";

Art Unit: 2136

7. Claim 5 ***additionally recites*** the limitations that “The method as recited in claim 1, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.”. The teachings of Bots et al (col. 6, lines 34-36, col. 8, lines 15-33, 45-63) suggest such limitations. Further, it would be inherent that for any table (list) oriented data structure, such as the said group/member database, the database entries would be the member elements themselves (i.e., member ID’s), and would be inherently of the same type (i.e., member ID types);

And further as per claim 28; “The network system [This claim is the apparatus of method claim 5, and is rejected for the same reasons provided for the claim 5 rejection above] as recited in claim 25, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.”;

And further as per claim 51; “The computer program product as recited in claim 47 [This claim is the software embodied on computer readable media for the method of claim 5, and is rejected for the same reasons provided for the claim 5 rejection above], wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.”.

8. Claim 6 ***additionally recites*** the limitations that “The method as recited in claim 5, wherein said ID type is an Internet Key Exchange (IKE) defined m type, wherein said list of members is a non-contiguous list of IKE defined ID types.”. The teachings of Bots et al (col. 6, lines 34-36, col. 8, lines 15-33, 45-63) suggest such limitations. Further, it would be inherent that for any table (list) oriented data structure, such as the said group/member database, the

Art Unit: 2136

database entries would be the member elements themselves (i.e., member ID's), and would be inherently of the same type (i.e., member ID types);

And further as per claim 29; "The network system [This claim is the apparatus of method claim 6, and is rejected for the same reasons provided for the claim 6 rejection above] as recited in claim 28, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.";

And further as per claim 52; "The computer program product as recited in claim 51 [This claim is the software embodied on computer readable media for the method of claim 6, and is rejected for the same reasons provided for the claim 6 rejection above], wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.".

9. Claim 7 *additionally recites* the limitations that "The method as recited in claim 5, wherein said ID is a login ID.". The teachings of Bots et al (col. 6, lines 34-36, col. 8, lines 15-33, 45-63) suggest such limitations. Further, it would be inherent that for any table (list) oriented data structure, such as the said group/member database, the database entries would be the member elements themselves (i.e., member ID's), and would be inherently of the same type (i.e., member ID types);

And further as per claim 30; "The network system [This claim is the apparatus of method claim 7, and is rejected for the same reasons provided for the claim 7 rejection above] as recited in claim 28, wherein said ID is a login ID.";



And further as per claim 53; “The computer program product as recited in claim 51 [This claim is the software embodied on computer readable media for the method of claim 7, and is rejected for the same reasons provided for the claim 7 rejection above], wherein said ID is a login ID.”.

10. Claim 8 ***additionally recites*** the limitations that “The method as recited in claim 5, wherein said ID is a specified name.”. The teachings of Bots et al (col. 6, lines 34-36, col. 8, lines 15-33, 45-63) suggest such limitations. Further, it would be inherent that for any table (list) oriented data structure, such as the said group/member database, the database entries would be the member elements themselves (i.e., member ID’s), and would be inherently of the same type (i.e., member ID types);

And further as per claim 31; “The network system [This claim is the apparatus of method claim 8, and is rejected for the same reasons provided for the claim 8 rejection above] as recited in claim 28, wherein said ID is a specified name.”;

And further as per claim 54; “The computer program product as recited in claim 51 [This claim is the software embodied on computer readable media for the method of claim 8, and is rejected for the same reasons provided for the claim 8 rejection above], wherein said ID is a specified name.”.

11. Claim 9 ***additionally recites*** the limitations that “The method as recited in claim 2, wherein configuring said tunnel definition database in said server node comprises establishing said server node and said client node as the two end points of said tunnel”. The teachings of Bots

Art Unit: 2136

et al (col. 5, lines 20-25, col. 7, lines 4-19, lines 32-39, lines 55-col. 8, line 4) suggest such limitations;

And further as per claim 55; “The computer program product as recited in claim 48 [This claim is the software embodied on computer readable media for the method of claim 9, and is rejected for the same reasons provided for the claim 9 rejection above], wherein configuring said tunnel definition database in said server node comprises: programming operable for establishing said server node and a client node as the two end points of said tunnel.”.

12. Claim 12 *additionally recites* the limitations that “The method as recited in claim 1, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.”. The teachings of Bots et al (col. 6, lines 34-36, col. 8, lines 15-33, 45-63) suggest such limitations. Further, it would be inherent that for any table (list) oriented data structure, such as the said group/member database, the database entries would be the member elements themselves (i.e., member ID’s), and would be inherently of the same type (i.e., member ID types);

And further as per claim 34; “The network system [This claim is the apparatus of method claim 12, and is rejected for the same reasons provided for the claim 12 rejection above] as recited in claim 25, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.”;

And further as per claim 58; “The computer program product as recited in claim 47 [This claim is the software embodied on computer readable media for the method of claim 12, and is

rejected for the same reasons provided for the claim 12 rejection above], wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.”.

13. Claim 16 *additionally recites* the limitations that “The method as recited in claim 1, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.”. The teachings of Bots et al (col. 2, lines 55-65, col. 7, lines 20-55, col. 8, lines 5-33, 45-63) suggest such limitations. Further, it would be inherent that for any table (list) oriented data structure, such as the said group/member database, the database entries would be the member elements themselves (i.e., member ID’s), and would be inherently of the same type (i.e., member ID types);

And further as per claim 38; “The network system [This claim is the apparatus of method claim 16, and is rejected for the same reasons provided for the claim 16 rejection above] as recited in claim 25, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.”;

And further as per claim 62; “The computer program product as recited in claim 47 [This claim is the software embodied on computer readable media for the method of claim 16, and is rejected for the same reasons provided for the claim 16 rejection above], wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.”.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

18. Claims 10-11, 32-33, 56-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bots et al, U.S. Patent 6,226,748 B1, as applied to claim 9, 26, 55, respectively, above, and further in view Shrader, U.S. Patent 5,864,666.

As per claims 10-11;

**(claim 10)** “The method as recited in claim 9, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID, and a remote ID type through a GUI.”. Shrader teaches of using a web based GUI, command line (col. 1, lines 15-34, col. 5, lines 13-col. 6, line 67) software application for IP tunneling (i.e., VPN architecture) *administration* (ABSTRACT, figures 4-7, and accompanying descriptions)

It would have been **obvious** to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Bots et al VPN invention, with the Shrader software application for IP tunneling (i.e., VPN architecture) administration, **because** it would allow a qualitative user interface improvement in such a distributed network environment for VPN administration (col. 1, lines 5-33);

**(claim 11)** “The method as recited in claim 9, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.”. Shrader teaches of using a web based GUI,

Art Unit: 2136

command line (col. 1, lines 15-34, col. 5, lines 13-col. 6, line 67) software application for IP tunneling (i.e., VPN architecture) administration (ABSTRACT, figures 4-7, and accompanying descriptions)

It would have been **obvious** to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Bots et al VPN invention, with the Shrader software application for IP tunneling (i.e., VPN architecture) administration, **because** it would allow a qualitative user interface improvement in such a distributed network environment for VPN administration (col. 1, lines 5-33);

As per claims 32-33;

**(claim 32)** “The network system [This claim is the apparatus of method claim 10, and is rejected for the same reasons provided for the claim 10 rejection above] as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.”;

**(claim 33)** “The network system [This claim is the apparatus of method claim 11, and is rejected for the same reasons provided for the claim 11 rejection above] as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.”;

As per claims 56-57;

**(claim 56)** “The computer program product as recited in claim 55 [This claim is the software embodied on computer readable media for the method of claim 10, and is rejected for the same reasons provided for the claim 10 rejection above], wherein said tunnel definition database in

Art Unit: 2136

said server node is configured by a user entering a local ID, a local ID type, said remote m and a remote ID type through a GUI.”.

*(claim 57)* “The computer program product as recited in claim 55 [This claim is the software embodied on computer readable media for the method of claim 11, and is rejected for the same reasons provided for the claim 11 rejection above], wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.”.

19. Claims 13-15,35-37,59-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bots et al, U.S. Patent 6,226,748 B1, as applied to claim 12,34,58, respectively, above, and further in view Shrader, U.S. Patent 5,864,666.

As per claims 13-15;

*(claim 13)* “The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI. ”. Shrader teaches of using a web based GUI, command line (col. 1,lines 15-34, col. 5,lines 13-col. 6,line 67) software application for IP tunneling (i.e., VPN architecture) administration (ABSTRACT, figures 4-7, and accompanying descriptions)

It would have been **obvious** to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Bots et al VPN invention, with the Shrader software application for IP tunneling (i.e., VPN architecture) administration, **because** it would allow a

Art Unit: 2136

qualitative user interface improvement in such a distributed network environment for VPN administration (col. 1, lines 5-33);

**(claim 14)** "The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface."

Shrader teaches of using a web based GUI, command line (col. 1, lines 15-34, col. 5, lines 13-col. 6, line 67) software application for IP tunneling (i.e., VPN architecture) administration (ABSTRACT, figures 4-7, and accompanying descriptions)

It would have been **obvious** to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Bots et al VPN invention, with the Shrader software application for IP tunneling (i.e., VPN architecture) administration, **because** it would allow a qualitative user interface improvement in such a distributed network environment for VPN administration (col. 1, lines 5-33);

**(claim 15)** "The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files."

Shrader teaches of using a web based GUI, command line (col. 1, lines 15-34, col. 5, lines 13-col. 6, line 67) software application for IP tunneling (i.e., VPN architecture) administration (ABSTRACT, figures 4-7, and accompanying descriptions). Further, the inherent use of configuration files in GUI (i.e., Windows 3.x ".ini.", and Windows 9x "registry" files ) is well known in the art.

It would have been **obvious** to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Bots et al VPN invention, with the Shrader software application for IP tunneling (i.e., VPN architecture) administration, **because** it would allow a qualitative user interface improvement in such a distributed network environment for VPN administration (col. 1, lines 5-33);

As per claims 35-37;

**(claim 35)** "The network system [This claim is the apparatus of method claim 13, and is rejected for the same reasons provided for the claim 13 rejection above] as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.";

**(claim 36)** "The network system [This claim is the apparatus of method claim 14, and is rejected for the same reasons provided for the claim 14 rejection above] as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface.";

**(claim 37)** "The network system [This claim is the apparatus of method claim 15, and is rejected for the same reasons provided for the claim 15 rejection above] as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.";

As per claims 59-61;



Art Unit: 2136

**(claim 59)** “The computer program product as recited in claim 58 [This claim is the software embodied on computer readable media for the method of claim 13, and is rejected for the same reasons provided for the claim 13 rejection above], wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.”.

**(claim 60)** “The computer program product as recited in claim 58 [This claim is the software embodied on computer readable media for the method of claim 14, and is rejected for the same reasons provided for the claim 14 rejection above], wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface.”.

**(claim 61)** “The computer program product as recited in claim 58 [This claim is the software embodied on computer readable media for the method of claim 15, and is rejected for the same reasons provided for the claim 15 rejection above], wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.”.

20. Claims 17-18,39-40,63-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bots et al, U.S. Patent 6,226,748 B1, as applied to claim 16,38,62, respectively, above, and further in view Shrader, U.S. Patent 5,864,666.

As per claims 17-18;

Art Unit: 2136

**(claim 17)** “The method as recited in claim 16, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a GUI.” Shrader teaches of using a web based GUI, command line (col. 1, lines 15-34, col. 5, lines 13-col. 6, line 67) software application for IP tunneling (i.e., VPN architecture) administration (ABSTRACT, figures 4-7, and accompanying descriptions)

It would have been **obvious** to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Bots et al VPN invention, with the Shrader software application for IP tunneling (i.e., VPN architecture) administration, **because** it would allow a qualitative user interface improvement in such a distributed network environment for VPN administration (col. 1, lines 5-33);

**(claim 18)** “The method as recited in claim 16, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a command line interface.” Shrader teaches of using a web based GUI, command line (col. 1, lines 15-34, col. 5, lines 13-col. 6, line 67) software application for IP tunneling (i.e., VPN architecture) administration (ABSTRACT, figures 4-7, and accompanying descriptions)

It would have been **obvious** to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Bots et al VPN invention, with the Shrader software application for IP tunneling (i.e., VPN architecture) administration, **because** it would allow a qualitative user interface improvement in such a distributed network environment for VPN administration (col. 1, lines 5-33);

As per claims 39-40;

Art Unit: 2136

**(claim 39)** “The network system [This claim is the apparatus of method claim 17, and is rejected for the same reasons provided for the claim 17 rejection above] as recited in claim 38, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a GUI.”;

**(claim 40)** “The network system [This claim is the apparatus of method claim 18, and is rejected for the same reasons provided for the claim 18 rejection above] as recited in claim 39, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a command line interface.”;

As per claims 63-64;

**(claim 63)** “The computer program product as recited in claim 62 [This claim is the software embodied on computer readable media for the method of claim 17, and is rejected for the same reasons provided for the claim 17 rejection above], wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a GUI.”.

**(claim 64)** “The computer program product as recited in claim 62 [This claim is the software embodied on computer readable media for the method of claim 18, and is rejected for the same reasons provided for the claim 18 rejection above], wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a command line interface.”.

***Allowable Subject Matter***

Art Unit: 2136

22. Claims 19-24,41-46,65-70 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims:

**(claim 19)** “The method as recited in claim 1 further comprising the step of: activating said tunnel, wherein activating said tunnel comprises the steps of sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.”;

**(claim 41)** “The network system as recited in claim 27, wherein activating said particular tunnel comprises the steps of: sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.”;

**(claim 65)** “The computer program product as recited in claim 47 further comprising: programming operable for activating said tunnel, wherein said programming operable for

Art Unit: 2136

activating said tunnel comprises: programming operable for of sending a security policy stored in a policy database of said client node by said client node to said server node; programming operable for sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node; programming operable for sending a first nonce by said client node to said server node; programming operable for sending a second nonce by said server node to said client node; programming operable for sending a first ID by said client node to said server node; and programming operable for sending a second ID by said server node to said client node.”.

**(claim 20)** “The method as recited in claim 19, wherein said first and second nonce are used to generate key material for said server and client node, respectively.”;

**(claim 42)** “The network system as recited in claim 41, wherein said first and second nonce are used to generate key material for said server and client node, respectively.”;

**(claim 66)** “The computer program product as recited in claim 65, wherein said first and second nonce are used to generate key material for said server and client node, respectively.”.

**(claim 24)** “The method as recited in claim 1 further comprising the step of: activating said tunnel, wherein activating said tunnel comprises the steps of: sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second

Art Unit: 2136

nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.”;

**(claim 46)** “The network system as recited in claim 27, wherein activating said particular tunnel comprises the steps of sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.”;

**(claim 70)** “The computer program product as recited in claim 47 further comprising: programming operable for activating said tunnel, wherein said programming operable for activating said tunnel comprises: programming operable for sending a security policy stored in a policy database of a client node by said client node to said server node; programming operable for sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node; programming operable for sending a first nonce by said client node to said server node; programming operable for sending a second nonce by said server node to said client node; programming operable for sending a first ID by said client node to said

Art Unit: 2136

server node; and programming operable for sending a second ID by said server node to said client node.”.

**(claim 23)** “The method as recited in claim 19, wherein said first ID is an ID of said particular member of said group name.”;

**(claim 45)** “The network system as recited in claim 41, wherein said first ID is an ID of said particular member of said group name.”;

**(claim 69)** “The computer program product as recited in claim 65, wherein said first ID is an ID of said particular member of said group name. ”.

**(claim 21)** “The method as recited in claim 19, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.”.

**(claim 22)** “The method as recited in claim 19, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.”.

**(claim 43)** “The network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.”;

**(claim 44)** “The network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

Art Unit: 2136

**(claim 67)** “The computer program product as recited in claim 65, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.”.

**(claim 68)** “The computer program product as recited in claim 65, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.”.

### ***Response to Amendment***

22. As per applicant's argument concerning Bots not disclosing configuring a server node group database, the examiner has fully considered the arguments and finds them not to be persuasive. The “group” is clearly defined and therefore configured as an inherent aspect of a VPN system with an operational VPN tunnel. Further, said ‘defined in a computer’ would also inherently encompass the *storage* of said definitions (Bots plural group definitions of plural VPN of groups), which would clearly be in a data base type of data structure (broadly interpreting the database definition, being that the specific type or nature of a specific database is not seen in the claim language).

Further, the applicant's argument concerning Bots not disclosing a server node per se, the examiner has fully considered the argument and find it not to be persuasive. The Bots VPN clearly operates as a server, with a server being a ‘source’ of data in a communications system (inclusive of a VPN), relative to a client ‘sink’ of data in such a network, this fact being independent of the data path (Bots VPN in-line with the data path). Also, the Bots VPNU clearly constitutes an at least an endpoint (node) in a network (i.e., part of the Internet, see



Art Unit: 2136

appropriate figure / description), and the VPNU's being configured would encompass that limitation.

23. As per applicant's argument concerning Bots not disclosing configuring a server node rules database, the examiner has fully considered the arguments and finds them not to be persuasive. The "rules" of the security policy of Bots is clearly defined and associated with the group designator (i.e., name) and therefore configured as an inherent aspect of a VPN system with an operational VPN tunnel. Further, said 'defined in a computer' would also inherently encompass the *storage* of said definitions (Bots plural group definitions of plural VPN of groups), which would clearly be in a data base type of data structure (broadly interpreting the database definition, being that the specific type or nature of a specific database is not seen in the claim language).

Further, the applicant's argument concerning Bots not disclosing a group name per se, the examiner has fully considered the argument and finds it not to be persuasive. The Bots VPN groups clearly are defined, and as discussed above, would have a designator, which clearly would constitute a "group name".

24. As per applicant's argument concerning Bots not disclosing a plurality of tunnels associated with a group name, the examiner has fully considered the arguments and finds them not to be persuasive. As discussed above, the VPN tunnels and group definitions so associated, are clearly part of a network of nodes in said network which clearly have appropriate network interfaces (hardware and software 'adapters', see appropriate figures).

25. As per applicant's argument concerning Bots not disclosing tunnel establishment with a commonly defined security policy, the examiner has fully considered the arguments and finds them not to be persuasive. As discussed above, the VPN tunnels and group definitions so associated, are clearly part of a network of nodes in said network which clearly has the security policy, as recited in the appropriate claim rejection above.

26. As per applicant's argument concerning Bots not disclosing the tunnel definition including node designation of the client as the remote ID designator, the examiner has fully considered the arguments and finds them not to be persuasive. The examiner broadly interpreting the claim language concerning the Bots lookup table, clearly allows for the equivalency of a lookup table data structure with a database type of structure.

27. As per applicant's argument concerning Bots not disclosing the ID types associations to group name and members, the examiner has fully considered the arguments and finds them not to be persuasive. The examiner broadly interpreting the claim language concerning the Bots lookup table, clearly allows for the equivalency of a lookup table data structure with a database type of structure inclusive of designators / descriptors (i.e., text, key type, etc.) that are inherently of a data structure type, allowing for an equivalency, as recited in the appropriate claim rejection above.

Art Unit: 2136

28. As per applicant's argument concerning Bots not disclosing the rules database comprising group name ID, ID type and security policy pointer (i.e., object reference), the examiner has fully considered the arguments and finds them not to be persuasive. The examiner broadly interpreting the claim language concerning the Bots lookup table, clearly allows for the equivalency of a lookup table data structure with a database type of structure inclusive of designators / descriptors (i.e., group name ID, ID type and security policy pointer, etc.) that are inherently of a data structure type, allowing for an equivalency, as recited in the appropriate claim rejection above.

29. As per applicant's argument concerning Bots not disclosing the ID and ID type of a login, IKE protocol descriptors / parameters, the examiner has fully considered the arguments and finds them not to be persuasive. The examiner broadly interpreting the claim language concerning the Bots lookup table, clearly allows for the equivalency of a lookup table data structure with a database type of structure inclusive of designators / descriptors (i.e., group name ID, ID type and security policy pointer, IKE type protocol descriptors, etc.) that are inherently of a data structure type, allowing for an equivalency, as recited in the appropriate claim rejection above.

30. As per applicant's argument concerning Bots and Shrader, taken singly or in combination, not disclosing the GUI, command line and configuration file user entry data system configuration, the examiner has fully considered the arguments and finds them not to be persuasive. The examiner broadly interpreting the claim language concerning the Bots lookup

Art Unit: 2136

table, clearly allows for the equivalency of a lookup table data structure with a database type of structure inclusive of designators / descriptors (i.e., group name ID, ID type and security policy pointer, IKE type protocol descriptors, etc.) that are inherently of a data structure type, allowing for an equivalency, as recited in the appropriate claim rejection above. Further, the obvious combination of the Shrader reference combines the GUI, command line and configuration file configuration aspects of the system setup for those appropriate parameters of the databases in the claims.

Further, as recited in the claims rejection language above, the databases are clearly configured, else they obviously could not properly be usable, therefore applicant arguments concerning the lack of teachings concerning configuration methods and procedures per se are moot.

31. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Art Unit: 2136

***Conclusion***

32. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

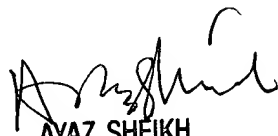
After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7246

Ronald Baum

Patent Examiner

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100